

A Dual Security Scheme using DNA Key based DNA Cryptography

Suman Phangal

Department Of Computer Sciences, TIT&S College,
Bhiwani, Haryana
India

Mukesh Kumar

The Technological Institute of Textile and Sciences,
Bhiwani, Haryana
India

Abstract: Cryptography is one of the most traditional and secure approach to provide reliable transmission over the web. The presented work is the improvement over the traditional symmetric cryptography approach by including the concept of DNA Sequencing. In this work, a two stage model is presented to improve the DNA Cryptography. This cryptography model uses the DNA Sequence as the Input Key to the system as well as uses the DNA object based substitution for cryptography. The work is applied on Images. The analysis of work is done under MSE and PSNR values. The obtained result shows the effective generation of cryptography image.

Keywords: DNA, Cryptography, MSE, PSNR, Secure

I. INTRODUCTION

Cryptography enables the data communication between two persons or between groups to provide secure communication over the network. This kind of communication not only prevents the unauthorized access over the network but also maintains the data integrity. The authentication is provided by digital signature or digital certificates. At the basic level cryptography approaches are divided in two main categorized based on numbers of keys involved in communication. These approaches are called private key cryptography and public key cryptography [1][2].

A) Symmetric Key Cryptography

This kind of cryptography approach is also called private key cryptography. As the name suggested in this cryptography approach only single key is involved to enable the encoding and decoding process. It means same key is used to perform data encryption and to retrieve the data back from cipher text. At the earlier stage, this kind of cryptography not looks stronger as the complete security depends on single key. But there are number of cryptography algorithms comes under symmetric key cryptography that increases the data integrity by using the larger key size and number of encoding level in the algorithmic approach. This is the most traditional type of cryptography, in which the key information is common for both sender and receiver. In such system, the sharing mechanism of key requires some effective approach. Single key is here defined to perform data encoding and decoding. This single key is able to provide the reliable communication over the network [3][4][5]. The cryptographic mechanism supported by this approach is shown in figure 1

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICTCS '14, November 14 - 16 2014, Udaipur, Rajasthan,
India Copyright 2014 ACM 978-1-4503-3216-
3/14/11...\$15.00 <http://dx.doi.org/10.1145/2677853.2677882>

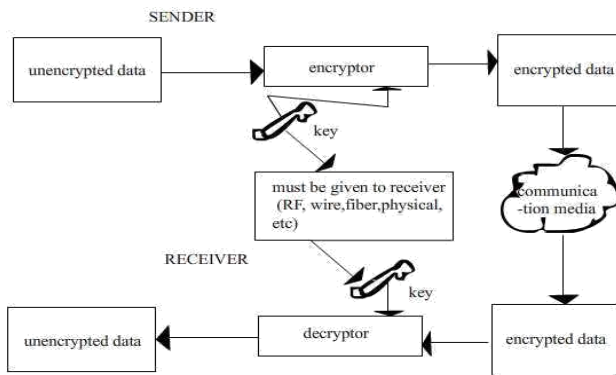


Figure 1: Symmetric Key Cryptography

As figure shows, the sender is having the raw information to transfer over the network. This raw information can be available in different media types. These media types can be textual information, image, videos etc. To perform the cryptography, the approach requires some algorithm called encryption and the key. This key is symmetric key shared between the senders as the receiver. As the cryptography algorithm is applied, the information is encoded to the cipher data form or called encoded information. Now this encoded information is transferred over the network. As the receiver receives the information it is in encoded form. Now the decryption is applied here to get the actual information back. The decryption uses the decoding algorithm and the same symmetric key to get the information data back. The security of this kind of algorithm depends on three main vectors called cryptography algorithm, key size and way to share the key. There are number of symmetric key cryptography algorithms such as DES (Digital Encryption Standard), Triple DES, AES (Advanced Encryption Standard) etc [6][7][8]. This algorithm provides the high level information security.

B) Public-Key Cryptography

This cryptography approach is also called asymmetric cryptography approach. According to his approach, encryption and decryption is performed by two different keys. As the encryption process begins, instead of generating single key, two keys are generated called Public key and Private Key. The generator A keeps the private key with him and distributes the public key to all users that can send information to it. Now, as some user B want to send information to the user A. In such case, user B will use the public key of User A to perform the encoding process. Here the cryptography will be performed using public key of receiver. Now after the encoded process, the cipher information is transferred to

the receiver A. As receiver receives this information, the decoding process is performed using private key of User A. This decoding process is able to get the information back in its original form [9][10][11].

C) DNA Sequencing

DNA itself defines the instruction code for genetic and by using it the protein structure of any living thing can be constructed or recomposed. Each DNA sequence ia based on four different bases called Adenine (A), cytosine (C), guanine (G) and Thymine (T). DNA sequence study is helpful to do the structural change or property change or behavior change for a particular living thing. To identify the characteristic match or to identify the similarity between two living things in terms of characteristics or the functionality or behavior, it is required to analyze them respective to their DNA sequence. Each DNA sequence is defined as the large information group that contains all kind of information about the living things. Such as if we take the example of wheat, it contains the information about the wheat color, smell, quality etc. If we have to find a particular quality of wheat among the wheat samples, the DNA sequence match for the particular pattern can be performed. Each pattern in DNA sequence represents the existing or non-existence of some characteristics or the behavior. But the identification of these patterns over the DNA sequence is a challenging task. In this present work, the main focus is to perform the identification of some of such patterns over the DNA Dataset Group.

In this paper, DNA based Symmetric Key cryptography approach is defined. Here, the symmetric Key is generated using DNA sequencing and DNA component based substitution is applied to perform the cryptography. In this section, the description of cryptographic algorithm is given along with exploration of public and private key cryptography. The section also defined the concept of DNA sequencing. In section II, the work defined by earlier researchers is presented. In section III, the proposed two stage model is defined to perform DNA cryptography using DNA sequence Key. In section IV, the results obtained from the work are presented and discussed. In section V, the conclusion obtained from the work is presented.

II. EXISTING WORK

Lot of work is already done by different researchers to improve the information security under different media types and under different communication system. Some

of the efforts of earlier researchers are discussed in this section.

In year 2012, Ohood S. Althobaiti, discuss the relationship between cryptography and mathematics in the context of Elliptic Curve (EC). Author presents the idea of biometric signature - a new method to combine biometrics with public key infrastructure (PKI), the security can be increased using the ECC in biometric signature creation, because the private and public keys are produced without saving and sending any secret information anywhere[1]. In Year 2012, Seny Kamara defined a work on Symmetric encryption using dynamic searchable technique. The presented approach allows a client to encrypt the data in such way the search can the data can be performed over it. Author has defined SSE based scheme to satisfy the search condition. The work presented by the author actually extends the inverted index approach in different non-trivial ways and also introduce new technique to design the SSE. Author implemented the presented scheme and conducts the performance evaluation. The presented approach is highly efficient and ready for the deployment [2]. In year 2011, Parisa Kaghazgaran presented a work on to the provided the information security in case of involvement of more than one party in encryption process. Author defined the variant of comparison problem under different input. Author presented the work in real time situations where the cryptography is required. Author presented the cryptography at protocol level and provides the comparative analysis on existing and modified secure protocol approach for data encoding. Author enabled the secure transmission over the network [3].

Trisha Chatterjee presented a work on the cryptographic algorithms for symmetric key cryptography. Author provided more secure approaches by modifying the existing symmetric key cryptography approaches. The modification is here done at cipher text generation. Author provided the new algorithm to provide the text based encoding at the frequency level analysis. Author enabled the ASCII character encoding to perform the cryptography and to convert the information one form to other. This cryptography approach is based on random key generation [4]. Another work on visual information cryptography using the DH scheme was proposed by Chao-Wen in year 2008. Author presented an improved mechanism based Diffie-Helman approach for visual cryptography approach. Author used a shared key mechanism using visual cryptography. Author used the half tone shadow images to show the work implementation. Author implemented the work using shared key and symmetric key approaches to achieve

high level security [5]. Another work on block cipher cryptography and white box cryptography to secure the data was performed by Jaesung Yoo in year 2012. In this paper, Author implemented an improved AES for image encryption by using the dynamic key updating approach. Author adopted composite mode using White-Box AES and Standard AES. Presented scheme shows almost same performance with Standard AES and provides dynamic key approach effect. Moreover, it has a CPA-secure property and can be constructed for CCA-secure scheme with Message Authentication Code [6]. Wasim A Al-Hamdani defined a work on Elliptic Curve Cryptography to protect the data. Author defined a public key based approach under the algebraic structure. This was performed on a smaller group can be used to obtain the same level of security as RSA based. In this article a simple presentation on cryptography with focus on elliptic curve algorithm, examine its security, benefits and its functions with privacy issues [7].

A work on identity based cryptography was performed on symmetric cipher cryptography by Joonsang Baek. In this paper, as contributions to this line of research, Author construct hybrid identity-based encryption schemes which produce compact cipher texts while providing both efficiency and strong security without resorting to the strong length preserving symmetric cipher. In this paper, author defined a comparative analysis under different communication attacks to reveal the communication information and to extract the user data under different assumptions. Author provided the symmetric key encryption under improved form [8]. Another work on Symmetric encryption with key exchange scheme to achieve the computational soundness. In this paper, Author presented an improved mechanism for key sharing on the network. Author defined a new improved protocol to enable the public key cryptography and to provide the secure key sharing over the network [9]. A work on Homomorphism encryption scheme was proposed by Craig Gentry. Author propose a fully homomorphism encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Presented solution comes in three steps. Author improved the existing public key cryptography approach by included the ideal lattices. Author defined time bound mechanism to improve the integrity under time frame based key sharing. Author also used a hierarchical approach to enable the secure information encryption and sharing without specifying the conditional data transmission over the network. Author secures the private information communication under secure means. The presented key assignment scheme also improves the security in terms of cryptography approach [10]. Ueli

Maurer performed a work on authentication based scheme using symmetric encryption. Author highlight two reasons for investigating nevertheless AtE as a general paradigm: First, this calls for a definition of confidentiality; what separates a confidential from a secure channel is its (potential) malleability. Author proposes the first systematic analysis of malleability for symmetric encryption, which, in particular, allows us to state a generic condition on encryption schemes to be sufficient for AtE [11].

III. PROPOSED MODEL

Image cryptography actually deals in the image pixels under some defined mechanism. One of such common approach is the changing the pixel pattern by performing some pixel transformation approach. According to this approach, the pixels are switch from one position to other under some defined mechanism. These mechanisms include the translation, rotation etc. As the pixels are transformed, the new pixel values are not able to present the information clearly and the encoded image is obtained. In this work, an effective image cryptography model is presented based on DNA sequencing. Here the concept of DNA sequencing is defined at two levels. The proposed DNA based cryptography model is shown in figure 2.

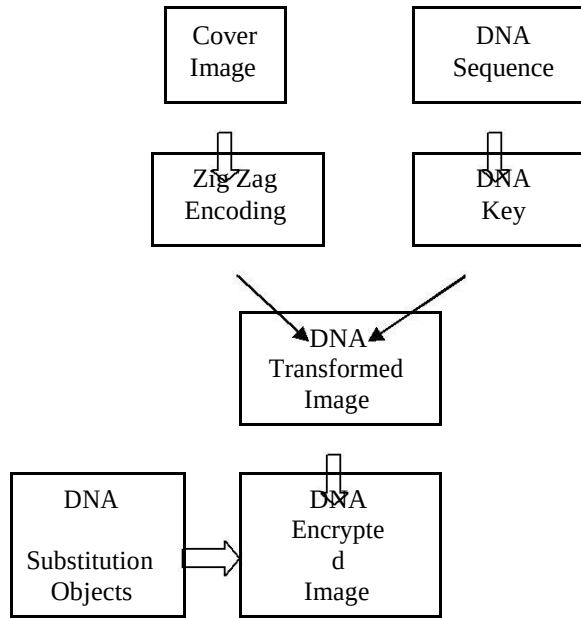


Figure 2: Proposed Model

Here figure 2 is showing the cryptographic model for input image by including the concept of DNA key. The largest DNA sequence pattern is identified over the input

pattern to use it as DNA sequence key. Once the key is generated, the next work is to encode the input image using Zig Zag Sequencing. This obtained sequence is then combined DNA key by using mathematical operator and it will generate the encoded image based on DNA sequencing. Once the transformed image is obtained, the next work is to obtain the bit sequence from the image. To perform the DNA cryptography, the DNA characters are defined with relative binary substitution. These binary substitution values are replaced over the bit sequence of DNA transformed image. Based on this substitution, the DNA cryptographic image will be obtained as the final result.

A) DNA Sequencing

The key concept associated with this presented work is the generation of DNA sequence pattern. This pattern is used the DNA key for symmetric key cryptography. To generate this key, the DNA sequence is taken as input and some pattern mining operation is applied over the sequence. In this work, the DNA sequence mining is applied to obtain the largest pattern sequence over the DNA sequence. This obtained sequence key is used as the actual DNA key based on which the DNA transformed image is generated. The algorithmic approach applied to obtain the largest pattern key is shown in table 1

Table 1: DNA Key Generation Algorithm

```

Algorithm(DNASeq)
/*DNASeq is taken as the input sequence to obtain the
largest sequence pattern over the sequence. This
largest size pattern is used as the input key for DNA
cryptography*/
{
  1. For i=1 to length(DNASeq)
    [Process the DNA Sequence]
    {
  2. Define the DNA Pattern of size j over
    the sequence
  3. Freq(z)=Count(DNASeq,
    DNAPattern) Seq(Z)=DNAPattern
    Z=z+1
    [Find the DNA Pattern frequency over
    the sequence]
    }
  4. Index=Max(Freq)
    [Find the maximum frequency pattern over
    the sequence]
  5. Return Seq(Index)
}
  
```

B) Zigzag based Encoding

Once the largest frequency DNA sequence is obtained. This sequence is used as the key for DNA transformed Image generation. To generate this image, the input image is encoded using Zigzag pattern as shown in figure 3.

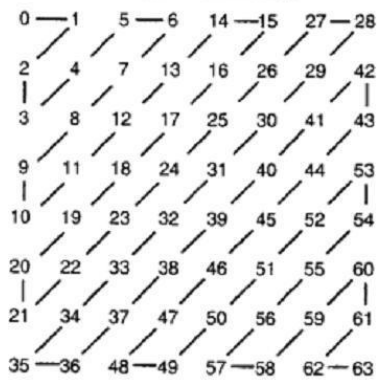


Figure 3: Zigzag Pattern Sequence

As the input image is encoded using some pattern sequence generation. The sequence is generated using 8 Bit ASCII codes. Once this sequence is obtained, it is presented in the form of vector. This sequence vector is combined with repetitive DNA sequence key by using the mathematical operator. Once the inclusion of this input pattern is done to the Encoded image sequence, the DNA encoded image is generated.

C) DNA Object Substitution Cryptography

At the final stage of work, the DNA cryptograph is applied on DNA encoded image. To perform this cryptography, the DNA characters are assigned with specific 2 Bit binary codes. These codes are shown in table 2.

Table 2 : DNA Encoding Codes

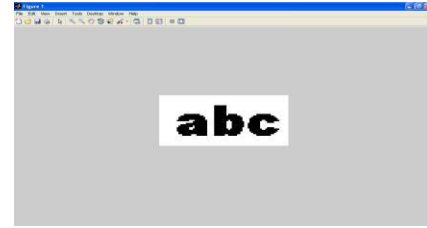
DNA Character	Binary Code
A	00
G	01
T	10
C	11

After the specification of these codes, the DNA encoded image is also transformed to binary codes. Now these codes are grouped in two bit codes and the substitution of these binary codes is done in terms of DNA characters. Based on this substitution of binary codes, the final cryptographic DNA encoded object is generated. This

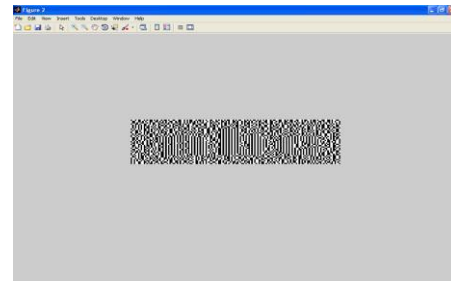
DNA sequence is then transformed in the form of image as the final result to represent the encoded object image.

IV. RESULTS

The presented work is implemented in mat lab environment. The work is applied on real time images. The DNA sequence is extracted from web sources to generate the DNA key. The analysis of work is defined under different parameters. The parameters included in this work are MSE, PSNR and correlation values. The sample image on which the cryptography is applied is shown



4 (a): Input Image



4(b): Encoded Image Figure 4: Input and Encoded Image

The work is tested on multiple input images. The results obtained from the work under different parameters is shown in table 3

Table 3: Analysis Parameters

Image	PSNR	MSE	Correlation
1.jpg	34.56	18.23	.0678
2.jpg	43.35	14.45	.235
3.jpg	33.23	22.64	.456
4.jpg	44.34	19.34	.145
5.jpg	33.23	14.23	.323

The graphical represents of results is shown in figure 5.

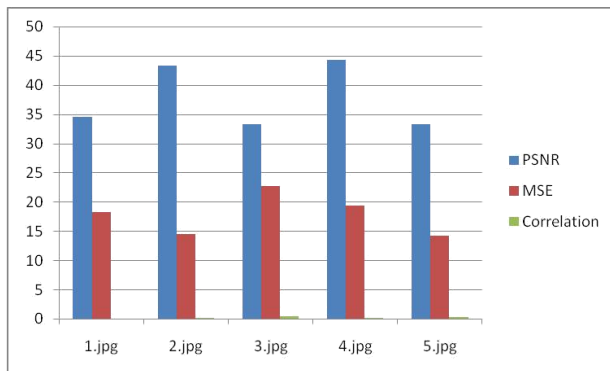


Figure 5 : Analysis Results

The obtained results shows, the presented work is effective in terms of obtained PSNR and MSE values.

V. CONCLUSION

In this paper, a DNA based symmetric key cryptography approach is presented. In this work, DNA sequencing is applied at two stages. In first stage, DNA sequencing is used to generate the key and at second stage, DNA is used to perform the cryptography. The work is applied on real time images. The analysis of work is done under MSE, PSNR and correlation vectors that show the satisfactory outcome from the work.

References

- [1] Ohood S. Althobaiti, an Enhanced Elliptic Curve Cryptography for Biometric, 7th International Conference on Computing and Convergence Technology (ICCCT), pp 1048–1055, 2012
- [2] Seny Kamara, Dynamic Searchable Symmetric Encryption, CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 965-976)
- [3] Parisa Kaghazgaran, Secure Two Party Comparison over Encrypted Data, World Congress on Information and Communication Technologies, pp 1127-1130, 2011
- [4] Trisha Chatterjee, Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm, Information and Communication Technologies (WICT), pp 1179, 2011
- [5] Chao-Wen Chan, A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme, IJCSNS International Journal of Computer Science and Network Security, Vol.8 Issue.4, pp 128-132, April 2008
- [6] Jaesung Yoo, A Method for Secure and Efficient Block Cipher using White-Box Cryptography, Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, 2012
- [7] Wasim A Al-Hamdani, Elliptic Curve for Data protection, Proceedings of the 2011 Information Security Curriculum Development Conference, pp 1-14, 2011
- [8] Joonsang Baek, Compact Identity-Based Encryption without Strong Symmetric Cipher, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp 61-70, 2011
- [9] Ralf Kusters, Computational Soundness for Key Exchange Protocols with Symmetric Encryption, Proceedings of the 16th ACM conference on Computer and communications security, pp 91-100, 2009
- [10] Craig Gentry, Fully Homomorphism Encryption Using Ideal Lattices,, Proceedings of the 41st annual ACM symposium on Theory of computing, pp 169-178, 2009
- [11] Giuseppe Ateniese, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, International Association for Crypto logic Research, pp 288-297, 2006